



Tax season is here: Avoid the “Dirty Dozen” Tax Scams!

UC Davis Information Security Office wants campus affiliates to review the Internal Revenue Service annual “[Dirty Dozen](#)” list of tax scams. The IRS emphasizes that they “continue to see scam artists use the pandemic to steal money and information from honest taxpayers in a time of crisis.” The IRS estimates that identity thieves have stolen billions via tax fraud. Don’t become another victim!

Be on the alert for:

- Any message asking for W-2 or other tax information.
- Authentic looking emails impersonating UC or UC Davis communications about accessing your W-2.
- Messages that look like they are from executive management requesting copies of employee W-2s for review purposes.
- Messages with links that encourage you to click on them, offer you something for nothing, or threaten you.
- Any message asking for your user ID or passwords.
- Unexpected phone calls about tax information or charitable donations or calls asking you to install software.
- Messages using keywords such as “coronavirus,” “COVID-19” and “Stimulus.”

Protect yourself:

- To access your W-2 statement, visit the University of California UCPATH website via [MyUCDavis](#) portal instead of clicking on a link in an email.
- Use a different way to validate any request for W-2 or other tax information, even if it looks like a legitimate request. For example, if you receive an email, call the person to verify.
- Do not reply to emails asking for your password or SSN.
- Familiarize yourself with the [IRS’ “Dirty Dozen” tax scams](#) so you recognize them.

Additional Information: [IRS Tax Scams/Consumer Alerts](#)